iStorage®

CLOUDASHUR®

De sleutel tot uw data



VERSLEUTEL

om ultieme bescherming van uw opgeslagen data in de cloud of op uw lokale PC/MAC te verzekeren

DEEL

uw versleutelde data veilig met geautoriseerde gebruikers in de cloud, via e-mail en real-time bestandsoverdrachtdiensten

BEHEER

en controleer uw cloudAshur apparaten centraal

Om data privacy te bewerkstelligen is encryptie van gegevens belangrijk en beveiliging van de encryptiesleutel essentieel. Voor een echt veilige oplossing is het dringend noodzakelijk dat de encryptiesleutel apart van de data wordt bewaard.

Dit is waarom wij de cloudAshur Hardware Security Module (patent aangevraagd) hebben ontwikkeld. Een door een PIN code geverifieerde hardware versleutelde beveiligingsmodule, die alle data in transfer en alle statische data versleutelt met een FIPS gecertificeerde willekeurig gegenereerde AES 256-bit versleutelde encryptiesleutel. Deze encryptiesleutel wordt opgeslagen in een speciale iStorage microprocessor (CC 4+ Ready).

OVERZICHT

cloudAshur is de perfecte oplossing voor iedereen die veilig gegevens in de cloud wil opslaan, delen, beheren en controleren. cloudAshur elimineert beveiligingsrisico's op cloud platforms zoals gebrek aan controle en ongeautoriseerde toegang. Hackers verzinnen diverse geraffineerde methodes gericht op onschuldige en kwetsbare gebruikers. Menselijk falen is ook een veelvoorkomende oorzaak van datalek-incidenten.

De consequenties van een gehackte cloud account kunnen diefstal en het lekken van vertrouwelijke gegevens zijn, hetgeen potentieel verlies van banen, negatieve publiciteit, forse boetes en de ondergang van een bedrijf kan betekenen.

iStorage software suite

cloudAshur Client app *(Windows & macOS)*

cloudAshur is compatibel met zowel PC's, MAC's en werkt met talloze cloud providers zoals Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud en nog vele anderen.

cloudAshur KeyWriter app *(Windows)*

iStorage KeyWriter (patent aangevraagd) maakt het delen tussen geautoriseerde gebruikers van data in de cloud, via e-mail en middels bestandsoverdrachtdiensten (bijv. WeTransfer) tot een koud kunstje. Met ultieme beveiliging en gemoedsrust kunnen gebruikers veilig real-time gegevens met elkaar delen, ongeacht waar zij zich bevinden.

cloudAshur Remote Management app *(Windows)*

De iStorage cloudAshur Remote Management console geeft u volledige controle over alle cloudAshur hardware beveiligingsmodules binnen uw organisatie hetgeen uitgebreide functionaliteiten biedt voor het beheren en monitoren van alle gebruikers.

All trademarks and brand names are the property of their respective owners.

All about IT Security E-QUIPMENT

CLOUDASHUR®



CLOUD ENCRYPTIE MODULE FUNCTIES

PINcode geverifieerde en hardware versleutelde cloud encryptie module (patenten aangevraagd)

Ultra-veilige 7-15-cijferige PIN ter authenticatie van de cloudAshur module.

Crypto-chip op het apparaat

Biedt 100% real-time militaire gradatie AES-XTS of AES-ECB 256-bit Hardware Encryptie met FIPS PUB 197 gecertificeerde USB 3.0 encryptie controller.

Brute force anti-hack verdedigingsmechanisme

Als de gebruikerspincode 10 keer achter elkaar foutief wordt ingevoerd, wordt de pincode verwijderd en kan de schijf alleen worden geopend door de Admin PIN in te voeren om zo de gebruikerspincode opnieuw in te stellen. (De Admin kan deze standaard ingestelde 10 foutieve PIN-pogingen wijzigen naar 1 tot 9 PIN-pogingen, alleen voor de desbetreffende gebruiker).

Als de Admin PINcode 10 keer achter elkaar foutief wordt ingevoerd dan gaan alle PINcodes en de versleutelde encryptiesleutel voor altijd verloren.

Vijf factor authenticatie

Iets dat u heeft:

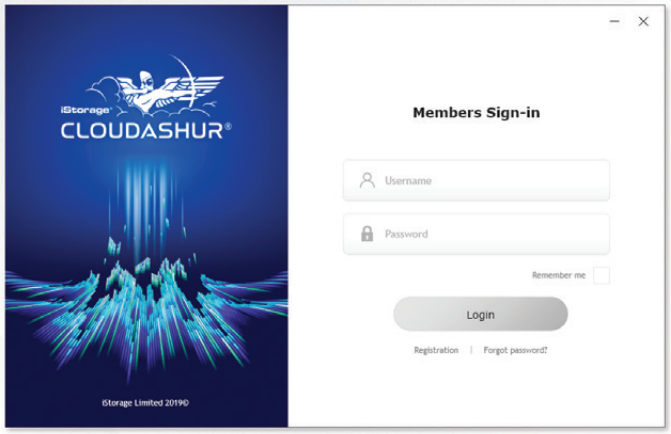
1. *De cloudAshur hardware beveiligingsmodule.*

Iets dat u weet:

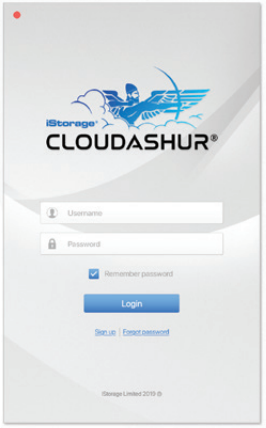
2. *7-15 cijferige Admin/Gebruikers instelbare PIN*
3. *Gebruikersnaam en wachtwoord voor de iStorage cloudAshur Windows of macOS client app*
4. *Waar de data is opgeslagen, welke cloud provider*
5. *Gebruikersnaam en wachtwoord voor de cloud account*

Compatibel met Windows en macOS

cloudAshur client applicaties zijn Windows (7/8/10) en macOS (Sierra/High Sierra/Mojave) compatibel.



(Windows Client App)



(macOS Client App)

Twee encryptiemethodes

De cloudAshur kan worden geconfigureerd in twee encryptiemethodes: AES-ECB 256-bit (FIPS Compliant) en ES-XTS 256-bit.

FIPS Level 3 compliant fraudebestendig & evident ontwerp

Alle kritische componenten van de cloudAshur behuizing zijn bedekt met een laag van extreem sterk epoxyhars dat nauwelijks is te verwijderen zonder de kritische componenten permanent te beschadigen. Wordt er toch geprobeerd 'in te breken' dan zal het fraudebestendige ontwerp van de cloudAshur module duidelijke sporen van geknoei en beschadiging vertonen.

Bevat unieke Common Criteria EAL4+ ready secure microprocessor

Biedt ultieme beveiliging tegen hackers, signaleert en reageert op fraude en inbreuk op functionaliteiten zoals:

- *Speciale hardware ter beveiliging tegen SPA/DPA/ SEMA, DEMA aanvallen*
- *Geavanceerde bescherming tegen fysieke aanvallen zoals Active Shield, Enhance Protection Object, CStack checker, Slope Detector and Parity Errors*
- *Environmental Protection Systems beschermend tegen spanningsmonitor, frequentiemonitor, temperatuurmonitor en lichtbescherming.*
- *Veilig Geheugen Manaement/Toegangsbescherming*

All trademarks and brand names are the property of their respective owners.

All about IT Security
E-QUIPMENT

CLOUDASHUR®

CLOUD ENCRYPTIE MODULE FUNCTIES

Polymeer omhuld, slijtvast on-board alfanumeriek toetsenbord

De cloudAshur wordt geauthenticeerd (ontgrendeld) en alle functies worden uitgevoerd door gebruik van het on-board toetsenbord zonder tussenkomst van een hostcomputer.

cloudAshur is niet kwetsbaar voor key-loggers en brute force aanvallen. Het cloudAshur toetsenbord is omhuld met een laag slijtvast polymeer ter extra bescherming.

Whitelisting op netwerken

Geconfigureerd met een unieke VID/PID en intern/extern serienummer met barcode, voor gemakkelijke integratie met standaard end-point management software (white-listing), om aan interne bedrijfsvereisten te voldoen.

PIN inschrijving voor de gebruiker

De Admin kan een restrictiebeleid voeren voor de gebruikersPIN. Dit omvat het instellen van een minimale PINcode lengte en indien nodig ook het verplicht invoeren van een of meer 'Speciale Karakters'.

'Speciale Karakter' functies zoals 'SHIFT (⇧) +cijfer'

Automatisch Slot bij Inactiviteit

Instelbaar slot bij vooraf bepaalde periode van inactiviteit. cloudAshur gaat automatisch op slot bij verwijdering uit de hostcomputer of wanneer er geen stroomvoorziening meer is naar de USB-poort.

Immuun voor BAD USB

Zowel de USB Cryptochip als de Secure Microprocessor bevatten digitaal ondertekende geheugenslot mechanismen die de cloudAshur immuun maken voor BAD USB.

Klantspecifieke mogelijkheden beschikbaar

Biedt een in-house PIN configuratie en laser-graveerservice waarbij de de cloudAshur hoes of zijkant van de module kunnen worden bedrukt met uw naam, bedrijfsnaam, logo, website/e-mailadres en telefoonnummer.

IP58 gecertificeerd

Stof- en waterbestendig. Bevat hard geanodiseerd en robuuste, geëxtrudeerde aluminium beschermingshoes.

Aparte Admin- en Gebruikers instellingen

Ondersteunt onfhankelijke Admin- en GebruikersPINcodes.

Zelfvernietigingsmogelijkheid

Programmeer de cloudAshur vooraf met een zelfvernietigings-PIN, die, wanneer ingetoetst, de versleutelde encryptiesleutel en alle PIN-codes in een keer wist.

Eenmalige Gebruikersherstel-PINcode

De Admin kan de cloudAshur instellen met een eenmalige herstel-PINcode. Dit is erg handig als de gebruiker de PINcode is vergeten om de cloudAshur te verifiëren.

Deze optie stelt de gebruiker in staat de herstel-PINcode in te voeren en een nieuwe gebruikers PIN-code in te stellen.

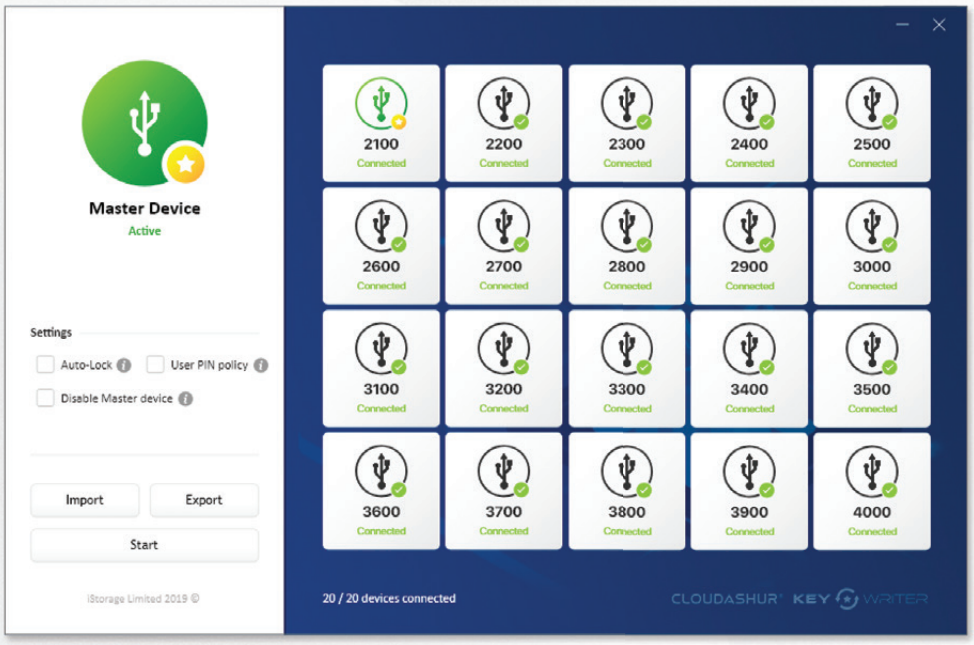


All trademarks and brand names are the property of their respective owners.

All about IT Security E-QUIPMENT

CLOUDASHUR KEYWRITER (PATENT AANGEVRAAGD)

Maakt het delen van data in de cloud, via e-mail en d.m.v. bestandsoverdachtdiensten tussen geautoriseerde gebruikers tot een koud kunstje met ultieme beveiliging en gemoedrust!



KEYWRITER FUNCTIES

- *iStorage KeyWriter kopieert alle kritische beveiligingsparameters inclusief de willekeurig gegenereerde encryptiesleutel en alle PINcodes tussen de Master cloudAshur module én alle vereiste slave cloudAshur modules bij gebruik van elke USB hub, hetgeen geautoriseerde gebruikers in staat stelt veilig en real-time data met elkaar te delen, ongeacht waar zij zich bevinden.*
- *De kritische beveiligingsparameters blijven altijd op de cloudAshur module staan en zijn opgeslagen in de Common Criteria EAL4+ ready secure microprocessor.*
- *Het proces van kopiëren van de versleutelde encryptiesleutel en alle kritische toegangsgegevens tussen de Master cloudAshur module en de slave cloudAshur modules wordt beschermd met een veiligheidsprotocol dat is verankerd in de iStorage cloudAshur secure microcontroller. Het protocol is geïmplementeerd door middel van cryptografische algoritmes die allemaal FIPS gecertificeerd zijn. Elke cloudAshur heeft een uniek betrouwbaarheidscertificaat dat verzekert dat alleen iStorage cloudAshur modules kunnen worden gebruikt tijdens het sleuteluitwisselingsproces.*
- *De cloudAshur modules geven nooit de vastgestelde sessie-sleutel prijs tijdens het uitvoeren van het veiligheidsprotocol en de gevoelige gekopieerde data wordt alleen ontsleuteld in de gevalideerde ontvangende cloudAshur module. De iStorage KeyWriter software die op de PC draait, coördineert de door het veiligheidsprotocol vereiste operaties, de software heeft echter geen zicht op de sessiesleutel noch op de ontsleutelde data. Dit maakt het voor een hacker onmogelijk om toegang te krijgen of kritische veiligheidsparameters te achterhalen die zijn opgeslagen in de cloudAshur module.*

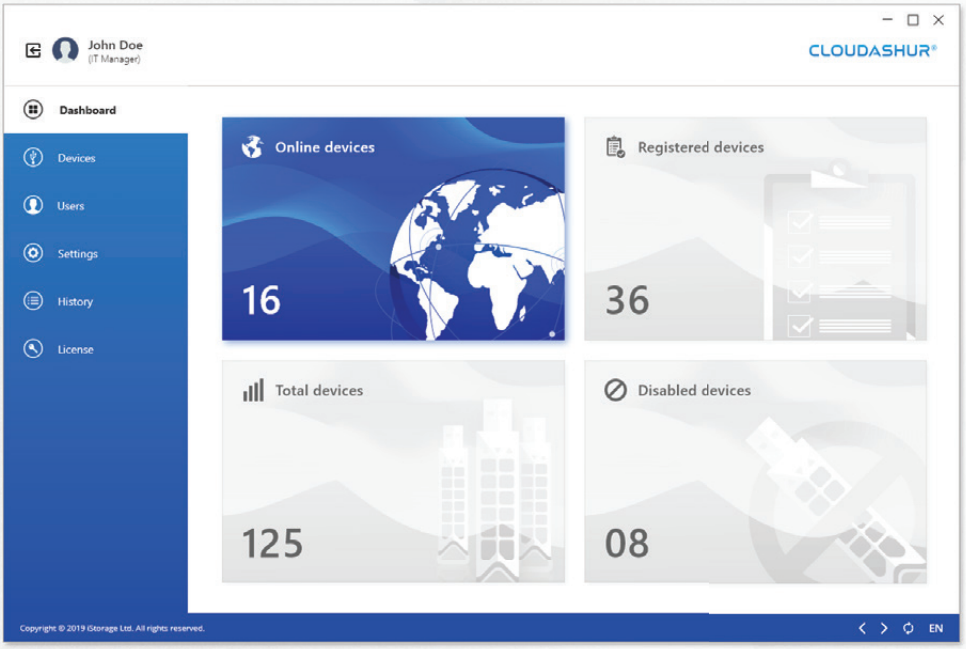
iStorage KeyWriter is compatibel met Windows (*Vista/7/8/10*).

All trademarks and brand names are the property of their respective owners.

All about IT Security E-QUIPMENT

CLOUDASHUR REMOTE MANAGEMENT CONSOLE

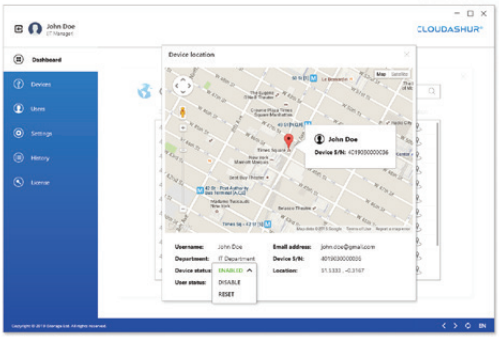
Geeft u volledige controle over alle cloudAshur hardware beveiligingsmodules binnen uw organisatie, dit biedt diverse functionaliteiten om alle gebruikers te beheren.



CONSOLE FUNCTIES

iStorage Remote Management Console geeft de Administrator volledig zicht en controle over het volgende:

- *Tijdelijk onbruikbaar maken of opnieuw instellen (op afstand) van gebruikers cloudAshur modules – in geval van verdachte activiteit of werknemer die organisatie verlaat zonder cloudAshur encryptie module in te leveren.*
- *Bestandstypes beperken – controleer welke bestandstypes worden geüpload en gedeeld in de cloud (EXE, PNG, PDF, etc....)*
- *Bekijk logbestanden van gebruikers– volledig inzicht in wat elke gebruiker doet in de cloud, zoals welke bestanden zij uploaden, downloaden, aanpassen etc..*
- *Toon locatie van de gebruiker – U kunt de locatie van de cloudAshur modules van de gebruiker zien via een map op uw scherm.*
- *Gebieds- en tijdsbegrenzing – beperk de tijd en locatie waarop de cloudAshur encryptie module kan worden gebruikt per individuele gebruiker.*



iStorage Remote Management Console is compatibel met Windows (Vista/7/8/10).

All trademarks and brand names are the property of their respective owners.

All about IT Security
E-QUIPMENT

WAAROM?

- *U bewaart de encryptiesleutel op de beste beveiligde manier mogelijk – u hoeft zicht niet langer zorgen te maken of uw data in de cloud wordt bekeken, gestolen of gedeeld.*
- *Vijf Factor Authenticatie – maakt het onmogelijk uw data te hacken.*
- *GDPR Compliance – De voorwaarden van grote cloud providers bevatten een "Beperkte Aansprakelijheids" clausule hetgeen de verantwoordelijkheid van de veiligheid van data bij de cloudgebruiker/klant legt, hoewel de data is opgeslagen op hun servers. Bijvoorbeeld, AWS verklaart in hun voorwaarden dat zij op geen enkele manier aansprakelijk zijn "bij ongeautoriseerde toegang tot, wijziging, verwijdering, vernietiging, verlies of het niet kunnen opslaan van uw data." cloudAshur geeft u ultieme bescherming. Als hackers toegang verkrijgen tot uw cloud account, zullen zij niet in staat zijn uw data te ontsleutelen.*
- *Mocht een hacker toch uw cloud login-gegevens verkrijgen door middel van "phishing" of andere geavanceerde hack methodes, zal de hacker niet in staat zijn uw data te ontsleutelen.*
- *Menselijk falen is niet langer een probleem.*
- *Bescherming tegen administratief personeel dat voor cloud providers werkt met mogelijke toegang tot uw data omdat zij de controle hebben over de encryptiesleutels.*
- *Bescherming tegen data privacy aspecten. Elk jaar worden door overheids-diensten tienduizenden aanvragen voor gebruikersdata verstuurd naar Google, Microsoft en andere bedrijven. In de meeste gevallen verstrekken deze bedrijven op z'n minst iets van data, zelfs al is het niet de volledige inhoud....*

TECHNISCHE SPECIFICATIES

Hardware	Hardware Security Module (patent aangevraagd)
Interface	FIPS PUB 197 gecertificeerde encryptie controller
Batterij	3.7V Li-Polymer oplaadbare batterij
Afmetingen - H/W/D	87.40mm / 19.40 mm / 13.40mm
Gewicht	Zonder hoes ca: approx. 28 grams Met hoes ca: approx. 37 grams
Compatibiliteit	cloudAshur is compatibel met zowel PC's als MAC's en werkt met talloze cloud providers zoals Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud en vele anderen.
Hardware data encryptie	Kan worden geconfigureerd in twee encryptie-instellingen AES-ECB 256-bit (FIPS Compliant) en AES-XTS 256-bit.
Certificeringen	FIPS 140-2 Level 3, NLNCSA BSPA & NATO Restricted Level (In aanvraag Q3/Q4)
Goedkeuringen	
Bestelinformatie	IS-EM-CA-256
Garantie	3 jaar garantie met gratis levenslange technische support



GDPR Compliant

Designed and Developed in the UK
Assembled in China

All trademarks and brand names are the property of their respective owners.